Diablo Canyon Power Plant Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," Revision 1 (Nonproprietary)

PACIFIC GAS & ELECTRIC COMPANY

DIABLO CANYON POWER PLANT

Topical Report:
Process Protection System Replacement
Diversity & Defense-in-Depth Assessment

Rev 1
August 2010

This page left blank by intent

Diablo Canyon Power Plant
Process Protection System Replacement
Diversity & Defense-in-Depth Assessment

Scott B. Patterson
Pacific Gas & Electric Company

John W. Hefler
Altran Solutions Corporation

Revision 1
August 2010

Pacific Gas & Electric Company
Diablo Canyon Power Plant
P.O. Box 56
Avila Beach, CA 93424

Record of Revisions

Revision Number	Affected Pages or Sections	Reason for Revision
0	All	Initial issue
1	1.0 2.0 Figure 2-8 2.3.2 2.3.3 1.0 3.1.4 3.1.5 3.2 3.4	Addressed USNRC RAI #1-8
	1.0 Table 2-1Title 2.2.2 3.1.1 3.1.51	Revised discussion to more closely reflect Eagle 21 SER Section 3.2 treatment of events where Eagle 21 PPS performed both primary and backup mitigation functions and where this evaluation determined that manual action was relied upon to mitigate some aspect of the events if a CCF were to occur concurrently.
	As marked	Miscellaneous editorial changes and clarifications

Table of Contents

Figures

Tables

1.0 Executive Summary

The Diablo Canyon Power Plant (DCPP) digital Eagle 21 Process Protection System (PPS) is being replaced to address obsolescence issues. The scope of the replacement is illustrated in the shaded portion of Figure 1-1.

A diversity study [2] performed for the original Diablo Canyon I&C system demonstrated that the analog protection and control design provided adequate diversity and defense-in-depth such that two or more diverse protective actions would terminate an accident before consequences adverse to public health and safety could occur.

The Safety Evaluation Report (SER) [13] for the Eagle 21 PPS shown in Figure 1-2 determined that automatic diverse means were available to mitigate all FSARU Chapter 15 accident or events that occurred with a concurrent postulated Common Cause Failure (CCF) to the PPS for events that:

1. Do not require the PPS for primary or backup protection;
2. Do not require the PPS for primary protection but assume PPS for backup protection; and
3. Require the PPS for primary protection but receive automatic backup protection from systems other than the PPS.

The following events require the PPS for both primary and backup protection for some aspect of the event. This evaluation has determined that these events would require manual operator action for mitigation if the event were to occur with a concurrent postulated CCF to the PPS.

1. Loss of forced reactor coolant flow in a single loop above P8 indicated by 2/3 reactor coolant flow-low;
2. Pressurizer pressure-low mitigation of Reactor Coolant System (RCS) depressurization, including Steam Generator Tube Rupture (SGTR), Steam Line Break (SLB) and Loss of Coolant Accident (LOCA); and
3. Containment pressure-high mitigation of Steam Line Break and LOCA.

The current NRC staff position regarding diversity and defense-in-depth (D3) to mitigate Chapter 15 accidents and events with a concurrent CCF is set forth in the Interim Staff Guidance (ISG) document from Task Working Group #2 [3] as follows:

> "When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty...

> "If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident...

The proposed replacement PPS [

Figure 1-3] addresses the ISG-02 staff position by: (1) implementing automatic protective functions in a Class IE software-based Triconex TRICON processor to mitigate events for which the Eagle 21 SER credited available diverse automatic mitigating functions; and (2) implementing automatic protective functions in a logic-based Class IE CS Innovations, LLC Advanced Logic System (ALS) that provides inherent, internal diversity to address software CCF per NRC ISG-02 [3] Position 1 and automatically mitigate events that otherwise would require manual protective action if the events were to occur with a concurrent CCF to the PPS [Refer to Section 2.3.2 for details].

The proposed replacement PPS ensures that the plant response to FSARU Chapter 15 accidents or events with a concurrent CCF is bounded by BTP 7-19 [14] acceptance criteria without the need for a unique Diverse Actuation System (DAS).

Figure 1-1 Westinghouse PWR Protection Scheme

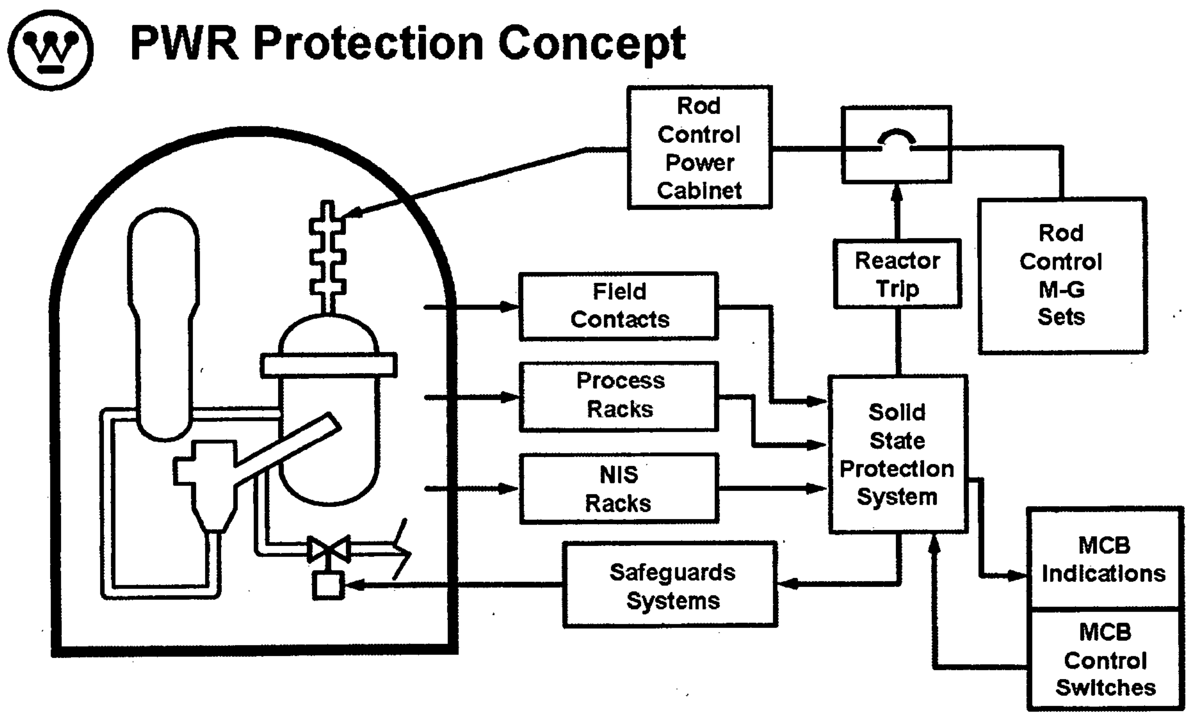


Figure 1-2 Existing Eagle 21 Process Protection System (PPS) Concept

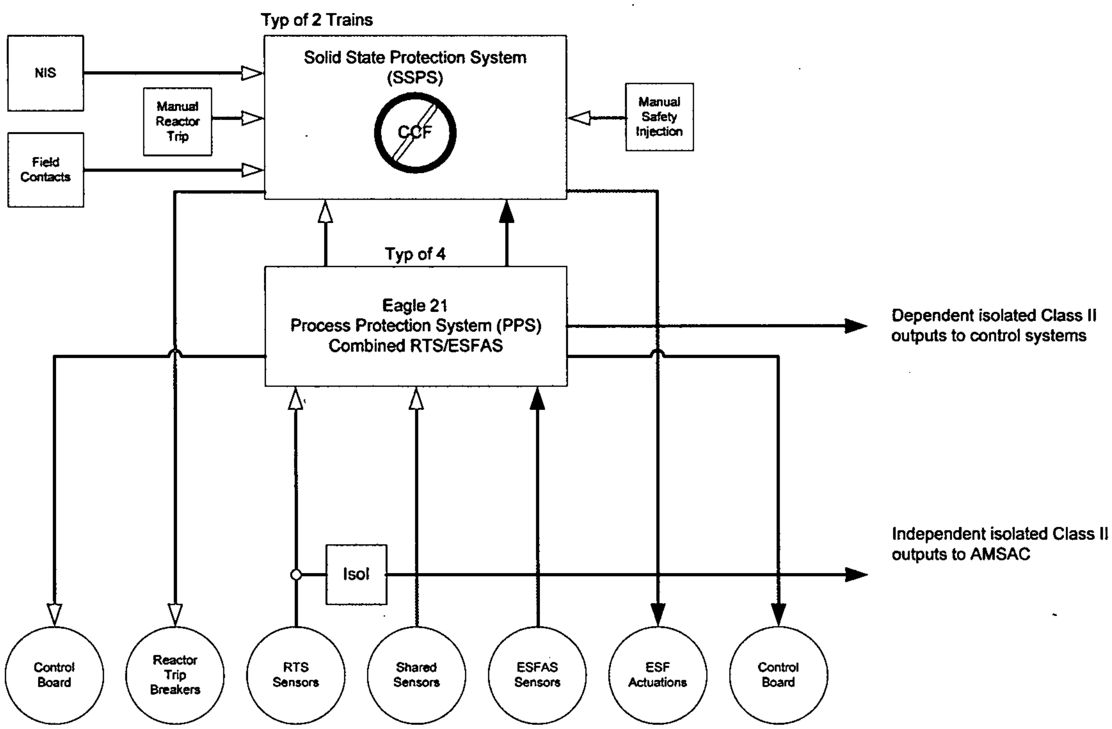


Figure 1-3 Replacement Process Protection System Concept

a

2.0 Diablo Canyon Process Protection System (PPS)

The existing digital Diablo Canyon Eagle 21 Process Protection System (PPS) monitors plant parameters, compares them against setpoints and provides signals to the Solid State Protection System (SSPS) if setpoints are exceeded. The SSPS evaluates the signals through coincident logic and performs Reactor Trip System (RTS) and Engineered Safety Features Actuation (ESFAS) command functions to mitigate an event that may be in progress.

The protection system is designed to provide two, three, or four process channels for each protective function and redundant (two) logic trains, as shown in Figure 2-1. Each individual process channel is assigned to one of four channel designations, e.g., Channel I,II, III, or IV. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel.

Redundant process equipment is separated by locating electronics in different protection rack sets. The four separate and redundant PPS rack sets (i.e., "Protection Sets") are comprised of Protection Racks 1-16.

Separation of the redundant process instrumentation channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks and then to the four SSPS input chassis of the two redundant SSPS logic racks ("Trains").

A process channel is defined as an arrangement of components, modules and software as required to generate a single protective action signal when required by a generating station condition [FSARU Section 7.1].

A protection set is defined as a physical grouping of process channels with the same channel designation. Each of the four redundant protection sets is provided with a separate and independent power feed and process instrumentation transmitters. Thus, each of the four redundant protection sets is physically and electrically independent from the other sets [FSARU Section 7.2].

A logic train is defined as one of the two sets of equipment that comprise the Solid State Protection System (SSPS). As shown in Figure 2-1, each of the two redundant and independent SSPS logic trains contains a logic cabinet and four separate input cabinets that receive trip signals from the PPS. Electronics in the logic cabinets perform coincident logic functions that actuate reactor trip and engineered safety system equipment based upon the PPS trip signals.

2.1 Reference Process Protection System (PPS)

Westinghouse I&C architecture uses several measurements of plant variables for both control and protection purposes. The functional capabilities required for control and protection are very similar and equipment suitable for one purpose is also suitable for the other, provided that qualified equipment is used to perform safety-related functions.

The original analog PPS, prior to addition of the AMSAC, is depicted in Figure 2-1. The analog PPS was designed to meet single failure criteria [10]. Functions generated by the analog PPS are illustrated in Figure 2-2.

2.1.1 Reference PPS Diversity and Defense-in-Depth

The Westinghouse design approach monitors numerous system variables by different means to provide functional diversity Westinghouse Topical Report WCAP-7306 [2] evaluated the diversity features provided by the original Westinghouse 7100 analog protection system architecture. The study considered effects of instrument channel failure across redundant protection sets.

WCAP-7306 considered effects of systematic or "common mode" failures that partially or completely prevent identical instrument channels from performing their function and demonstrated sufficient available diversity and defense-in-depth such that two or more diverse protective actions would terminate an accident without endangering public health and safety. For example, Large Break Loss of Cooling Accident (LBLOCA) was detected by Pressurizer Pressure – Low and Containment Pressure – High signals, either of which could initiate Engineered Safety Functions (i.e., Safety Injection) to mitigate the event.

The WCAP 7306 evaluation took credit for availability of two or more of the following "barriers" to demonstrate adequate diversity:

1. Tolerable consequence for the expected conditions (see below);
2. Low probability of accident;
3. Control interlocks that arrest the condition short of reactor trip; and
4. Manual action.

Depending upon the event and assumptions, event mitigation might not meet safety analysis goals, but sufficient margin was available to prevent endangering public health and safety. For example, Departure from Nucleate Boiling Ratio (DNBR) might decrease below the safety analysis limit, yet the consequences were still acceptable. Thus, the WCAP-7306 methodology predated today's "best estimate" evaluation methodology.

2.1.2 PPS Interfaces

In addition to its protection functions, the PPS provides process signals that are isolated from protection system sensors for use by various plant control systems. As shown in Figure 2-2, the control signals pass through the PPS, yet retain their identity from input through processing to output. A single failure in the PPS will not affect more than the control signals associated with the single failed channel.

Discrete bistable outputs from the PPS are routed to the Solid State Protection System (SSPS), which performs coincidence logic functions. Outputs from the SSPS actuate plant equipment in response to completed logic functions. Safety components, such as the Reactor Trip Breakers (RTB), pumps and valves may be actuated manually at both the redundant SSPS train level and at the component level using controls that are connected to the components downstream of the SSPS as shown in Figure 2-3 and Figure 2-4. The SSPS is not being modified for the PPS replacement project.

In this configuration, failures in the PPS cannot have an adverse impact on the operator's ability to exercise manual operation of reactor trip and ESF equipment at either the system or component level. The basic architecture described above was maintained when the Westinghouse 7100 PPS was replaced by Eagle 21. However, the Eagle 21 PPS is a software-based digital computer system in which certain primary and backup protective functions (e.g., Pressurizer pressure-low and containment pressure-high) are generated in the same platform and therefore are subject to a potential CCF that could disable both primary and backup protective functions [Refer to Section 2.2.2].

2.2 *Existing Eagle 21 Process Protection System (PPS)*

2.2.1 Eagle 21 Design

a

a

2.2.2 Eagle 21 Diversity and Defense-in-Depth (D3)

The Eagle 21 PPS Safety Evaluation Report (SER) [13] determined that sufficient diverse means were available to mitigate automatically all FSARU Chapter 15 accident or events that occurred concurrently with a postulated PPS Common Cause Failure (CCF) for:

1. Events that do not require the PPS for primary or backup protection;
2. Events that do not require the PPS for primary protection but assume the PPS for backup protection; and
3. Events that require the PPS for primary protection but receive automatic backup protection from systems other than the PPS.

The Eagle 21 PPS Safety Evaluation Report (SER) determined that the following events require the Eagle 21 PPS for both primary and backup protection for some aspect of the event. Diverse means of automatically mitigating the transient or plant indications (annunciators or indications) are available with sufficient procedural guidance for operators to diagnose the event in a timely manner and bring the plant to a safe shutdown condition.

1. Loss of forced reactor coolant flow
2. Accidental depressurization of the reactor coolant system
3. Loss of coolant accident (small- and large-break LOCA)
4. Steam line break (SLB) events
5. Steam generator tube rupture (SGTR)

Of the above events, the following would require manual operator action for mitigation if the event occurred concurrently with the postulated Eagle 21 PPS CCF:

1. Loss of forced reactor coolant flow in a single loop above P8 indicated by 2/3 reactor coolant flow-low;
2. Accidental RCS depressurization, including SGTR, SLB and LOCA indicated by Pressurizer pressure-low; and
3. Large Break LOCA and SLB indicated by Containment pressure-high.

2.3 *Proposed Replacement PPS*

The current NRC staff position regarding diversity and defense-in-depth to mitigate FSARU [1] Chapter 15 accidents and events with a concurrent CCF is set forth in the Interim Staff Guidance (ISG) document from Task Working Group #2 [3]. Conformance of the proposed replacement PPS to ISG-02 guidance is discussed in Section 1.0.

The proposed replacement PPS automatically performs the functions illustrated in Figure 2-7 using the architecture shown in Figure 2-8. PG&E does not propose to replace the diverse SSPS-based command portion of RTS/ESFAS, or the diverse Nuclear Instrumentation System (NIS) at this time. If AMSAC is replaced, the replacement system will be diverse from the protection system in accordance with 10CFR50.62 [9]. As shown in Figure 2-8, dedicated and independent isolation is provided for the AMSAC Narrow Range Steam Generator Water Level inputs. The AMSAC Turbine Impulse Pressure inputs are provided from non-safety-related signals that are diverse and independent from the PPS.

Process variables and trip functions for the replacement PPS are listed in the following tables.

Table 2-1 Process Variable Inputs for Tricon RTS/ESFAS Protection Functions

Process Variable	Protection Functions
Pressurizer Level	Pressurizer High-Level RT
RCS Narrow-Range Temperature	Input to OTDT RT
	Input to OPDT RT
	Input to SG Low-Low Level Trip Time Delay
Steam Generator Level	Steam Generator Low-Low Level RT
	Hi-Hi Level Feedwater Isolation
	Hi-Hi Level Turbine Trip
	Hi-Hi Level MFW Pump Trip
	Low-Low Level AFW Actuation (Process Sense performed by RTS; AMSAC utilizes independently isolated level signals and independent turbine impulse pressure channels to provide diverse function)
Steam Line Pressure	High-Negative Pressure Rate SLI
	Low-Pressure SI
	Low-Pressure SLI
Turbine Impulse Pressure	Permissive 13 Low Turbine Power Permissive (Input to P-7 Low Power Reactor Trip Permissive)

Table 2-2 Process Variable Inputs for ALS RTS/ESFAS Functions

Process Variable	Protection Functions
Pressurizer Pressure	Pressurizer Low-Low Pressure SI
	Pressurizer High-Pressure RT
	Pressurizer Low-Pressure RT
	Input to OTDT RT
Containment Pressure	High Pressure SI
	High Pressure (Phase A) Containment Isolation
	High Pressure (Phase B) Containment Isolation
	High-High Pressure Containment Spray
RCS Flow	RCS Low-Flow RT

Table 2-3 Diverse Protection Functions Not Affected by PPS Replacement

Process Variable	Protection Functions
Neutron Flux	Power-Range High-Flux (Low Setting) RT
	Power-Range High-Flux (High Setting) RT
	Power-Range Positive Flux Rate RT
	Power Range Flux Control Rod Stop
	Intermediate-Range High-Flux RT
	Source-Range High-Flux RT
	Input to OTDT RT
AMSAC (Steam Generator Low Level)	Turbine Trip Above C-20 Permissive/Reactor Trip Above Permissive 9
Main Turbine Stop Valve Position	Turbine Trip RT
Turbine Auto Stop Oil Pressure Low	
RCP Bus Undervoltage	RT
RCP Bus Underfrequency	RT
RCP Circuit Breaker Open	RT

a

a

2.3.1 Tricon-Based Replacement PPS Equipment

The TRICON is a mature commercial Programmable Logic Controller (PLC) that was designed from its inception for highly reliable use in safety systems. The TRICON has been shown by more than twenty years of experience to provide safe and reliable operation in safety critical applications. Triconex has more than 7,000 units in service and more than 410,000,000 operating hours without a failure to operate on demand.

High reliability and system availability is achieved through the triple modular redundant (TMR) architecture. This design enables the TRICON system to be highly tolerant to hardware failures, to identify and annunciate faults that inevitably occur, and to allow replacement of modules with the system online so that faults are repaired before they become failures.

Triconex issued a topical report to NRC as the basis for generic qualification of the TRICON PLC system for safety-related application in nuclear power plants [6]. Based on this submittal, NRC issued a SER for the platform [7] documenting staff findings that the platform possesses acceptable hardware and operating system software quality to be applied in safety-related RTS and ESFAS applications in nuclear power plants.

In September 2009, Triconex submitted a Topical Report [8] that was updated for the Version 10 Tricon as well as addressing current regulatory issues.

2.3.2 FPGA-Based Advanced Logic System (ALS) Replacement PPS Equipment

Where manual action is currently required to mitigate events that occur with a concurrent CCF to the PPS, automatic protective functions are generated in a diverse Class IE CS Innovations, LLC Advanced Logic System (ALS) [12]. The diverse ALS portion of the proposed replacement PPS is a logic-based platform that does not utilize a microprocessor and therefore has no software component required for operation of the system.

The FPGA is a hardware realization of a logic structure; that is, it is a programmable hardware logic device. An FPGA-based system does not use software in the traditional sense when it is in operation; however, its logic structure is generated (i.e., it is "programmed") in a manner similar to traditional software program development, with the same versatility and the same potential weaknesses.

The CS Innovations, LLC ALS application program development is structured to follow a traditional waterfall life cycle that includes a top-down requirement and specification development, design implementation, and a bottoms-up V&V effort at each level of integration. The ALS program development utilizes proprietary software tools that have been subjected to assessment and qualification. In-process quality assurance efforts are executed integral to the development stages, and a separate V&V team examines the outputs of each stage.

The ALS design practices and methodologies were accepted by NRC in their review and approval of the much simpler Wolf Creek Main Steam and Feedwater Isolation System (MSFIS) [11]. However, the MSFIS safety evaluation states that it is a unique application, and that future ALS applications, such as an RPS or ESFAS that receives input signals and makes trip decisions, may require additional design diversity.

Concern for ALS software CCF is addressed through incorporating additional design diversity in the FPGA-based hardware system and using qualified design practices and methodologies to develop and implement the hardware. The diverse ALS cannot be affected by a CCF that affects the Tricon. The proposed PPS provides sufficient design diversity to automatically mitigate Diablo Canyon FSARU Chapter 15 events where previous evaluations credited operator action should a CCF occur concurrent with the event. The ability of the ALS portion of the PPS to perform credited automatic protective functions is not affected adversely by software CCF. Therefore, the proposed design addresses Staff Position 1 of ISG-02 [3] adequately.

2.3.3 Preventing Protection/Control Interaction in the Replacement PPS

a

a

Figure 2-1 Original Westinghouse 7100 Analog Process Protection System (Before AMSAC)

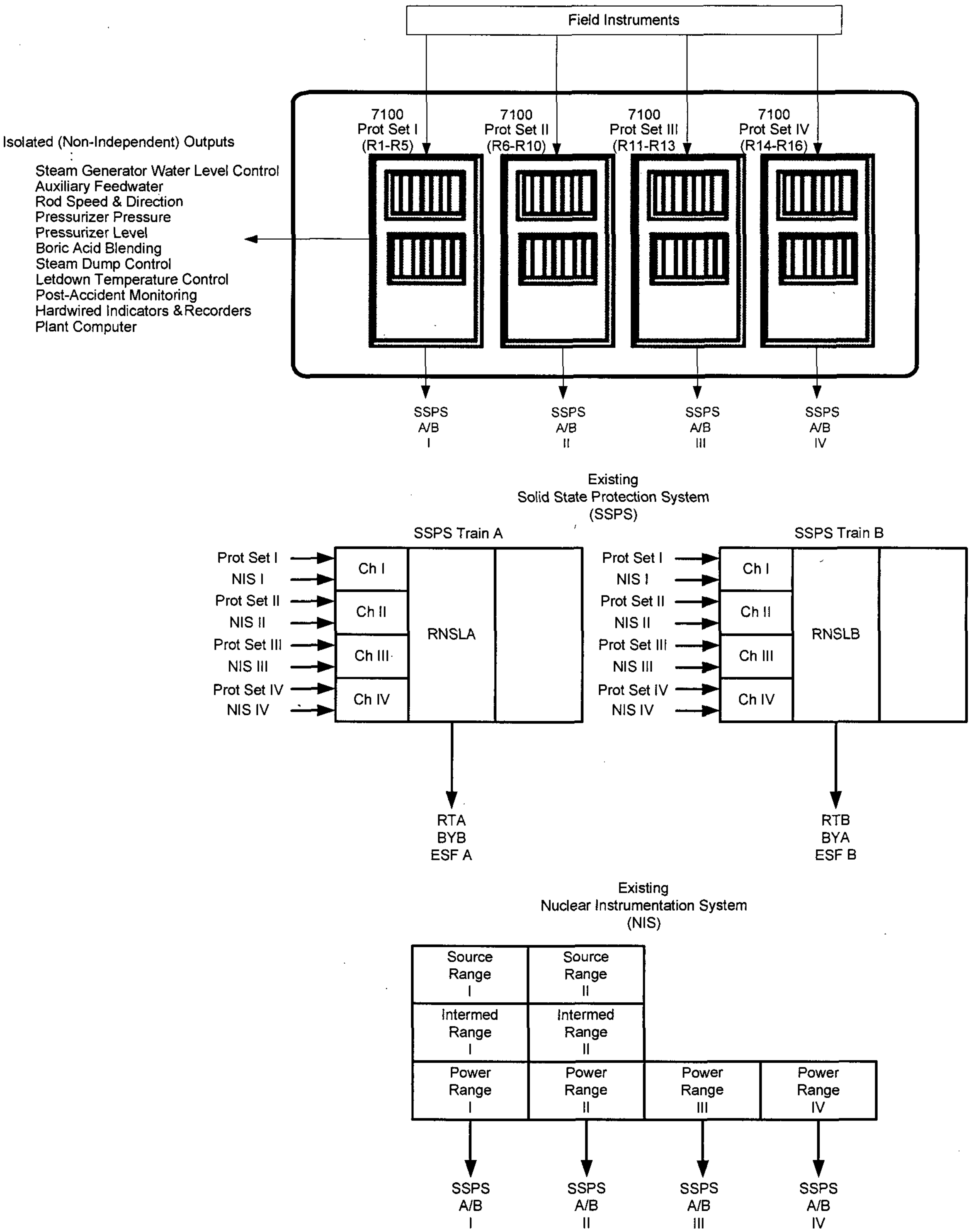


Figure 2-2 Westinghouse 7100 PPS Functions

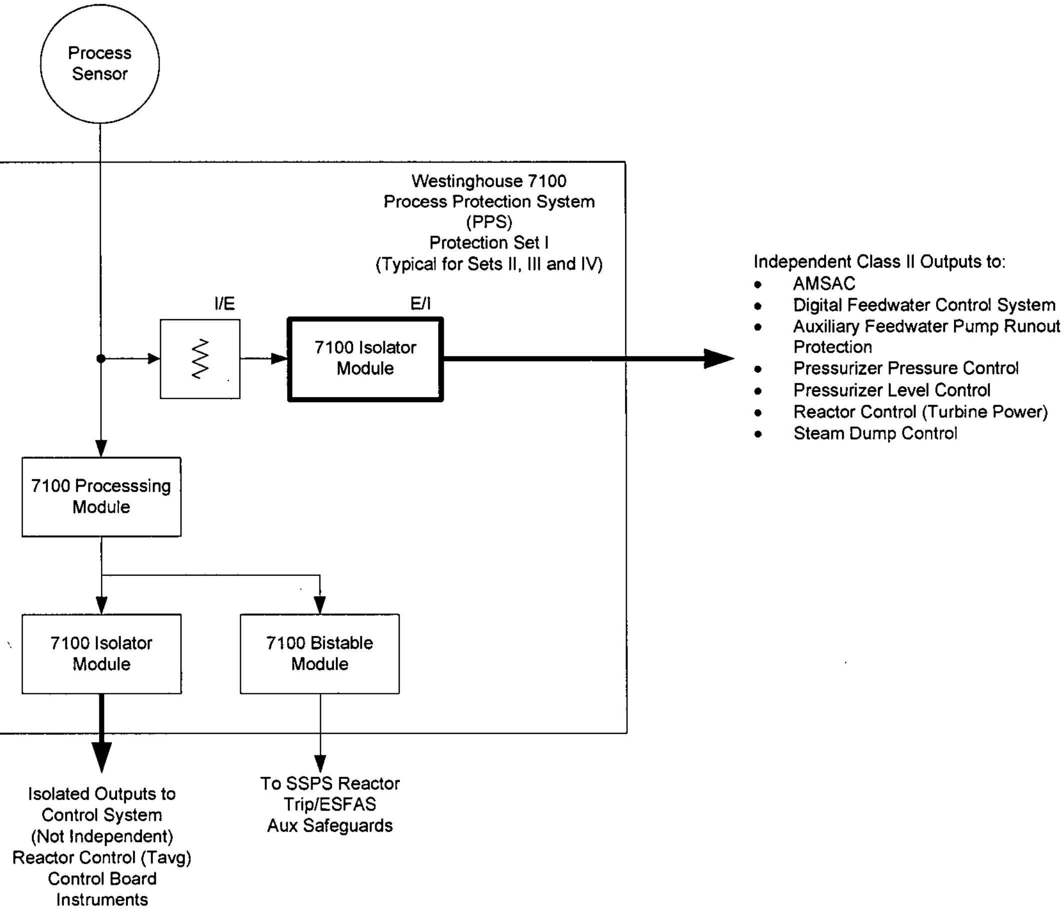
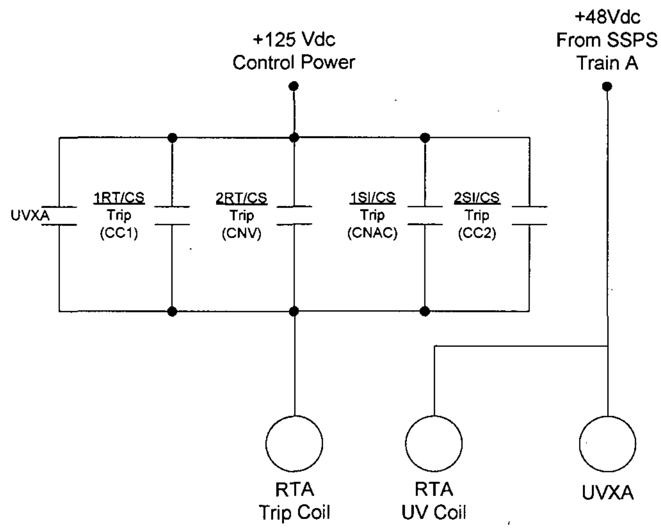
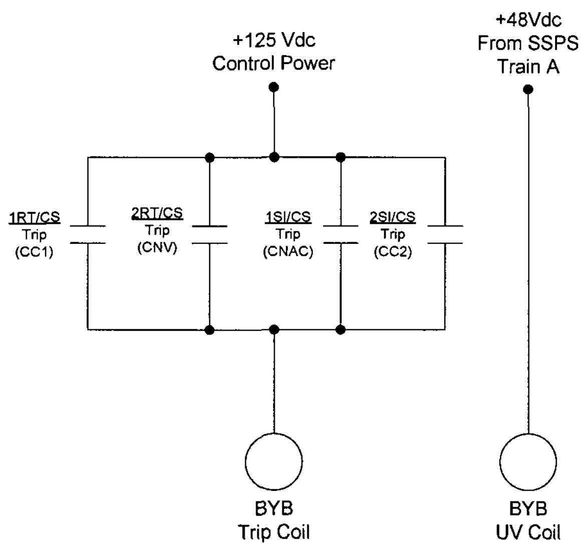


Figure 2-3 Reactor Trip Breaker Interface with RTS

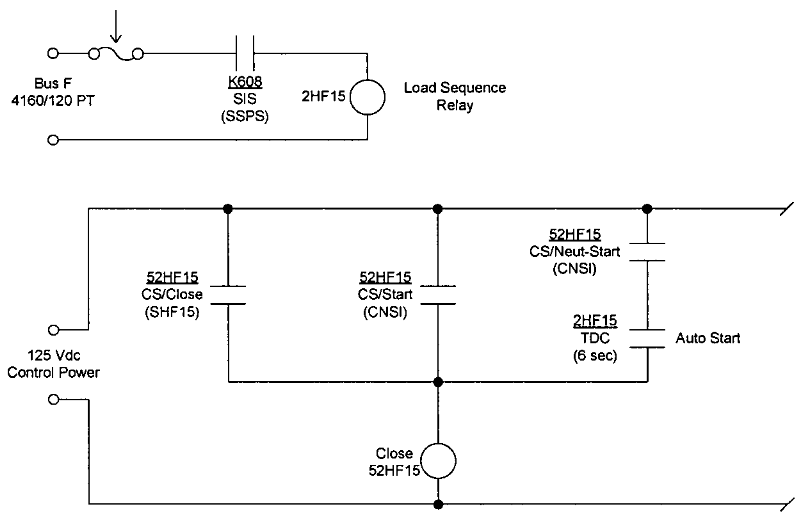


Reactor Trip Breaker A



Bypass Breaker B

Figure 2-4 Safety Injection Pump Interface with ESFAS



Circuit Breaker
52HF15
Unit 1 Safety Injection Pump 1

Figure 2-5 Eagle 21 Block Diagram

a

Figure 2-6 Typical Existing Eagle 21 PPS Functions

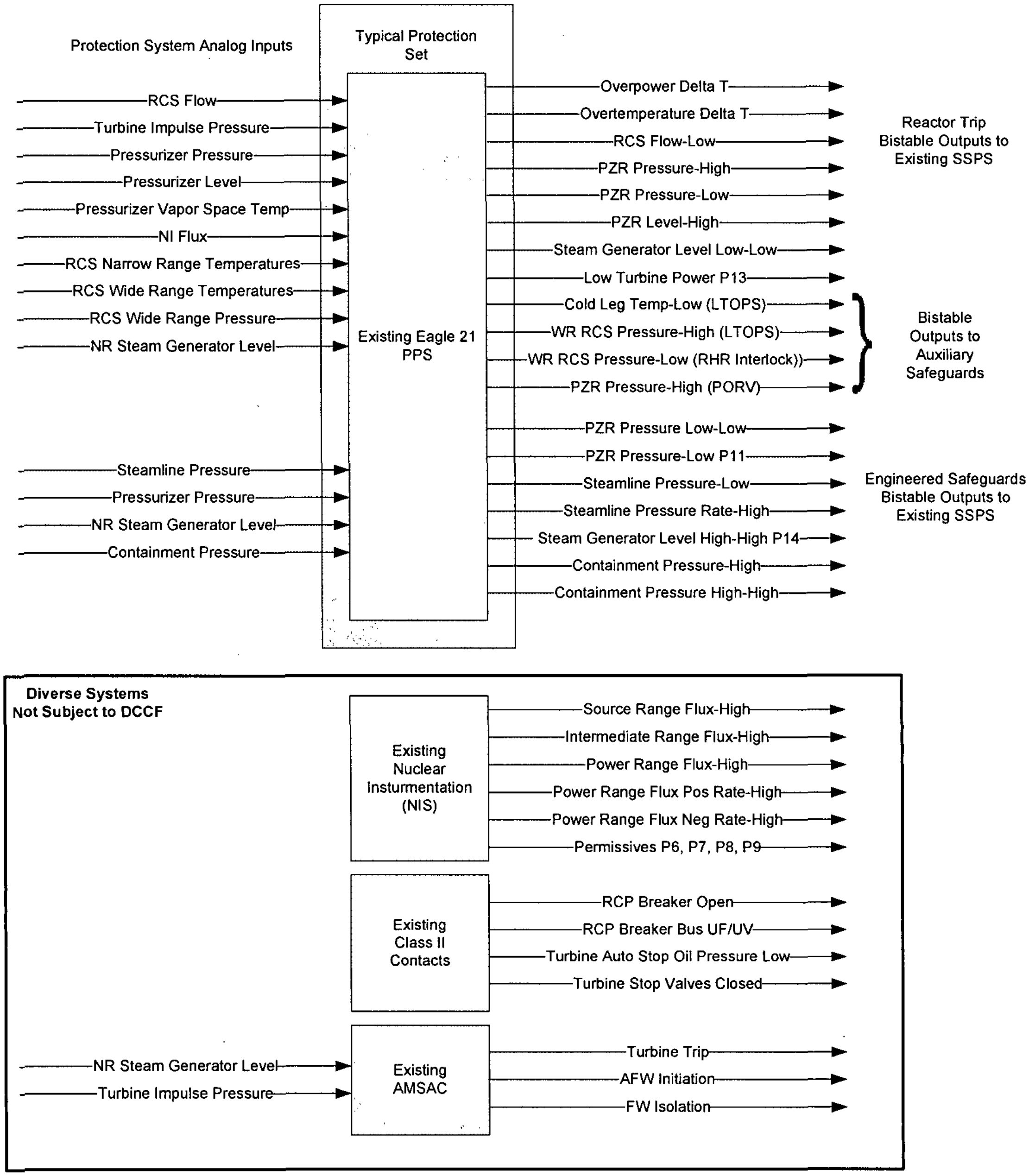


Figure 2-7 Typical Replacement PPS Functions

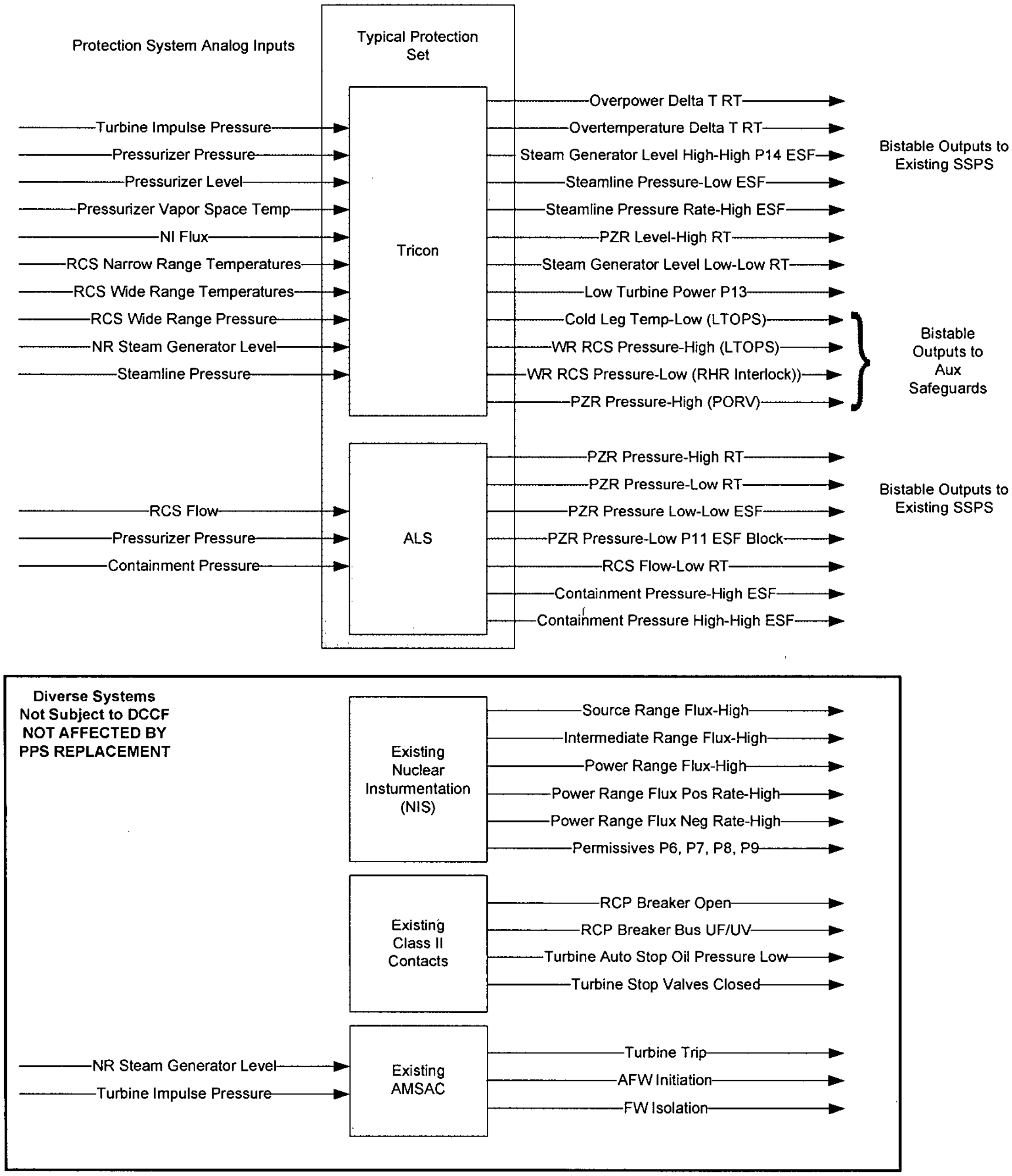


Figure 2-8 Replacement PPS Architecture Concept

a

This page left blank by intent

3.0 Diversity Evaluation of the Proposed Replacement PPS

If a postulated CCF can disable a safety function, BTP 7-19 [14] of the Standard Review Plan [5] Point 3 requires a diverse means, not subject to the same CCF to perform the same function or a different function. Credit may be taken for operator action; however, sufficient time must be available for the operator to diagnose the event and initiate mitigative action.

Section 3.1 of the NRC Eagle 21 SER [13] determined that diverse automatic measures existed to mitigate all FSARU Chapter 15 accidents and events that occur with a concurrent CCF, except for certain events where both the primary and backup mitigation functions were generated in Eagle 21. For the following events, plant indications and procedural guidance were relied upon for the operator to diagnose the event in a timely manner and bring the plant to a safe shutdown:

1. Loss of forced reactor coolant flow in a single loop above P8 indicated by 2/3 reactor coolant flow-low;
2. RCS depressurization, including Steam Generator Tube Rupture (SGTR), Steam Line Break (SLB) and Loss of Coolant Accident (LOCA) indicated by Pressurizer pressure-low; and
3. Large Break LOCA and SLB indicated by Containment pressure-high.

Interim Staff Guidance (ISG) 02 [3] describes the current NRC staff position regarding Diversity and Defense in Depth:

> "The licensee or applicant should perform a D3 analysis to demonstrate that vulnerabilities to CCFs are adequately addressed. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 1994 and Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," of NUREG-0800, "Standard Review Plan," describe an acceptable process for performing a D3 analysis...
>
> "When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty. Further, the licensee or applicant should provide sufficient information and controls (safety or non-safety) in the main control room that are independent and diverse from the RPS (i.e., not subject to the CCF).
>
> "If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within BTP 7-19 recommended acceptance

criteria for the particular anticipated operational occurrence or design basis accident.

"If manual operator actions are used as backup, a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions can be maintained within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident...

"In addition to the above guidance, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be unaffected by the CCF in the RPS. However, these displays and controls could be those used for manual operator actions as described above. Implementation of these manual controls should be in accordance with existing regulations.

For those events that relied on Eagle 21 for both primary and backup mitigation and thus required manual action by the operator in the event of a CCF to the Eagle 21 PPS, the replacement PPS provides Class IE automation that is not affected adversely by software CCF as described in Section 2.3.2.

The proposed automation performs accident mitigation functions to maintain plant conditions within the existing FSARU [1] Chapter 15 analyses of anticipated operational occurrences and design basis accidents. This approach is conservative with respect to the acceptance criteria recommended in BTP 7-19 [14].

3.1 *FSARU Chapter 15 Accidents and Events*

The purpose of the following discussion is to demonstrate that in the unlikely event of a common cause failure (CCF) of the proposed replacement PPS, coincident with an event analyzed as part of the Diablo Canyon Units 1 and 2 licensing basis, sufficient diverse means of mitigating the transient are available to bring the reactor to a safe shutdown condition.

The diversity of the proposed replacement PPS together with existing diverse protection functions, ensure that all FSARU Chapter 15 accident analysis acceptance criteria continue to be met in the event of software-related CCF concurrent with the accident or event. In most cases, if an accident were to occur, the plant initial conditions would be less severe than those analyzed for the FSARU. The AMSAC system, which is designed to provide protection against anticipated transients without reactor trip, is diverse and independent of the PPS and is not subject to a postulated CCF that disables the PPS.

Primary and backup protection system signals are provided for most of the transients comprising the Diablo Canyon licensing basis. For the purpose of this discussion, a primary protection signal is one upon which the protection function occurs in the licensing basis analysis. Backup protection signals are those expected to occur if the primary signal did not occur.

Where manual action was relied upon in previous evaluations to mitigate events that occurred with a concurrent CCF to the PPS , automatic protective functions are generated in the inherently diverse and independent CS Innovations, LLC Advanced Logic System (ALS) that is not affected adversely by software CCF as described in Section 2.3.2. Both the Tricon processor and the ALS are Class 1E, nuclear safety-related and perform all required safety functions that were approved by NRC in the Eagle 21 PPS Safety Evaluation Report [13].

The failure of Eagle 21 to provide an automatic protective function due to CCF was considered to be a beyond design basis failure mechanism and therefore was not incorporated into the FSARU Chapter 15 analysis of record accident analyses.

Table 3-1 identifies the primary and backup mitigating functions for each initiating event that is analyzed in Chapter 15 of the DCPP FSARU Update. These events represent the full set of events that need to be considered in assessing the impact of the digital modification on the accidents and events of FSARU Chapter 15.

The FSARU Chapter 15 licensing basis events and accidents listed in Table 3-1 may be divided into four categories per the Eagle 21 SER:

3.1.1 Events that do not require the PPS for primary or backup operation

In addition to the protection functions listed in Table 2-3 that are processed through systems other than the PPS, the following passive protection functions are assumed in several FSARU analyses.

1. Pressurizer Safety Valves
2. Steam Generator Safety Valves
3. Accumulators
4. Steam Line Check Valves

Table 3-2 summarizes events crediting these independent and diverse protective functions (Category 1 events). The analysis of these events either (1) takes credit for independent primary mitigating functions; or (2) does not require a primary mitigating function. The PPS functions listed as backup in the table provide additional backup to other independent and diverse backup functions. Therefore, mitigation of these events is completely unaffected by CCF of the PPS.

FSARU Section 15.3.4 Complete Loss of Forced Reactor Coolant Flow

A complete loss of forced reactor coolant flow may result from a simultaneous loss of electrical supplies to all reactor coolant pumps. The following functions mitigate a loss of coolant flow accident:

(1) Undervoltage or underfrequency on reactor coolant pump power supply buses

(2) Low reactor coolant loop flow

(3) Pump circuit breaker opening

The reactor trip on reactor coolant pump bus undervoltage protects against conditions that can cause a loss of voltage to all reactor coolant pumps, i.e., loss of offsite power. This function is blocked below Permissive 7 (approximately 10 percent power).

The reactor trip on reactor coolant pump underfrequency is provided to open the reactor coolant pump breakers and trip the reactor for an underfrequency condition, resulting from frequency disturbances on the major power grid. The trip disengages the reactor coolant pumps from the power grid so that the pumps flywheel kinetic energy is available for full coastdown. The hardware undervoltage/ underfrequency trip is generated independently of the PPS and is not subject to software CCF. This function is blocked below Permissive 7 (approximately 10 percent power).

The reactor trip on low primary coolant loop flow is provided to protect against loss of flow conditions that affect only one reactor coolant loop. For the complete loss of RCS flow event, it also serves as a backup to the undervoltage and underfrequency trips. This function is generated in the PPS by two-out-of-three low-flow signals per reactor coolant loop. Above approximately 35 percent power (Permissive 8), low flow in any loop actuates a reactor trip. Between approximately 10 and 35 percent power (Permissive 7 and Permissive 8), low-flow in any two loops actuates a reactor trip. Below Permissive 8, low flow in a single loop does not require a reactor trip.

A reactor trip from open pump breakers is provided as further backup to the low-flow signals. Above Permissive 7 a breaker open signal from any 2 of 4 pumps actuates a reactor trip. Reactor trip on reactor coolant pump breakers open is blocked below Permissive 7.

For the complete loss of forced reactor coolant flow, the FSAR analysis demonstrates that DNBR does not decrease below the safety analysis limit values during the transient, and thus, no core safety limit is violated. The hardware undervoltage/underfrequency trip function is generated independently of the PPS. Therefore, a diverse multiple loop loss of flow trip function is not required should the PPS fail due to CCF. Nevertheless, the low RCS flow function implemented in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS provides backup protection for this event. Replacement of the RPS enhances safety by providing a backup low RCS flow trip function.

The Pressurizer pressure-high reactor trip function, also generated in the inherently diverse ALS, provides additional diverse backup.

3.1.2 Events that do not require the PPS for primary but require the PPS for backup protection

Table 3-3 summarizes events that have primary protection that is independent of the PPS but require signals processed through the PPS for backup protection

(Category 2 events). The analysis of events discussed in this section is completely unaffected by CCF of the PPS since (1) the primary mitigating system responses are derived through systems other than the PPS; or (2) no protection system response is required for reactor and reactor coolant system protection.

3.1.3 Events that require the PPS for primary protection signals but receive automatic backup protection from systems other than the PPS

Table 3-4 summarizes events that assume the PPS for primary protection but have backup protection provided that is independent of the PPS (Category 3 events). These events receive primary protection system signals through the PPS and could be affected by a software related CCF to the PPS. However, backup protection signals are available that would automatically provide the necessary protection functions through systems other than the PPS.

With the exception of the single Rod Cluster Control Assembly (RCCA) withdrawal and feedline break events, all events in this category are classified as ANS Condition II events and have been analyzed by Westinghouse without reactor trip for Anticipated Transients Without Scram (ATWS) events. Above C-20 (40% rated thermal power, RTP), the AMSAC system is available to provide necessary protection functions. The AMSAC system initiates auxiliary feedwater and trips the turbine. Above Permissive 9 (50% RTP), the transients would be less severe than postulated for ATWS events, since an automatic reactor trip occurs independent of the PPS on turbine trip. Below C-20, generic analyses applicable to Diablo Canyon performed for ATWS events have demonstrated that the AMSAC is not required to prevent reactor coolant system damage.

3.1.4 Events that assume the PPS for primary and backup protection signals for some aspect of the automatic protection

Table 3-5 summarizes events that assume the PPS for primary and backup protection (Category 4 events), as well as diverse indicators and alarms derived through systems other than the PPS. These events receive both primary and backup protection signals for some aspect of the protection system response assumed in the safety analyses through the PPS. Table 3-5 also lists available diverse alarms, indicator lights, and recorders.

Where the Eagle 21 SER credited manual operator action to provide some of the necessary protection system functions should a CCF occur and disable the existing PPS, the replacement PPS provides automatic, independent and inherently diverse Class IE mitigation through the logic based ALS, which is not affected adversely by software CCF as described in Section 2.3.2. Steam Line Break events are included in this category since operator action otherwise would be required for feedwater isolation and safety injection. Backup reactor trip signals for steam line breaks occurring at power are provided via the Nuclear Instrumentation System.

3.1.5 Additional discussion of Category 4 Events (PPS Primary/PPS Backup)

The events discussed in this section receive both primary and backup protection signals for some aspect of the protection system response assumed in the safety analyses through the replacement PPS. Alarms, indicator lights, and recorders are available for these events that provides the operator with diverse indication of an event.

The Eagle 21 SER credited operator action to provide some of the necessary protection system functions should a CCF disable the Eagle 21 process protection system. These functions are generated automatically in the inherently diverse, independent Class IE ALS portion of the proposed replacement PPS. The diverse ALS is not affected adversely by software CCF as described in Section 2.3.2. Therefore, the mitigating functions occur when they are assumed to occur in the existing FSARU Chapter 15 analyses. It should be noted that in most cases various alarms/indicators would occur before a reactor trip or other protection system signal would have been generated by the replacement PPS.

The ALS portion of the replacement PPS automatically performs mitigative actions that were assumed in the Eagle 21 SER to be performed manually when the events occurred with a concurrent Eagle 21 CCF; these automatic mitigative functions occur sooner than the assumed manual actions; i.e., the mitigative functions continue to occur no later than assumed in the existing FSARU Chapter 15 accident analyses. Therefore, the plant response is bounded by BTP 7-19 [14] recommended acceptance criteria.

1. **Single Loop Loss of Forced Reactor Coolant Flow Events**

FSARU Section 15.2.5 Partial Loss of Forced Reactor Coolant Flow

Protection against a partial loss of coolant flow accident is provided by the lprimary coolant low flow reactor trip that is actuated by two-out-of-three low flow signals in any reactor coolant loop. The low flow signals are generated in the PPS. Above approximately 35 percent power (Permissive 8), low flow in any loop actuates a reactor trip. Reactor trip on low flow in 1 out 4 loops is blocked below Permissive 8. Between the power levels corresponding to Permissive 8 and approximately 10 percent power (Permissive 7) low flow in any two loops actuates a reactor trip. Reactor trip on low flow in two or more loops is blocked below Permissive 7. Diablo Canyon Technical Specifications do not require automatic reactor trip at these low power levels as discussed in FSARU [1] Section 7.2.1.1.2.2.

A reactor trip signal from the pump breaker position is provided as a backup to the low flow signal. When operating above Permissive 7, a breaker open signal from any two pumps actuates a reactor trip. Reactor trip on 2 out of 4 reactor coolant pump breakers open signal is blocked below Permissive 7. Additional backup protection is provided by RCP bus undervoltage and underfrequency. Although diverse and available, these functions do not provide automatic protection for single loop RCS loss of flow events.

The Eagle 21 SER does not explicitly describe mitigation of this event if the PPS fails due to CCF, and there is no backup to the PPS-generated RCS low flow trip functions to automatically mitigate this event.

In accordance with the guidance in NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the RCS Flow-Low reactor trip (2/3 Flow-Low in 2/4 loops > Permissive 7; 2/3 Flow-Low in any loop > Permissive 8) and the Pressurizer high pressure trip functions are generated in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

FSARU Section 15.4.4 Single Reactor Coolant Pump Locked Rotor

Automatic reactor trip functions and indications of a Locked Rotor event would be similar to the 1 out of 4 loop Partial Loss of Flow event. However, since the reactor coolant pumps have high inertia flywheels, the length of time for the flow to decrease would be significantly longer for a one-loop Partial Loss of Flow event than it would be for a Locked Rotor event.

Indications of a one-loop Partial Loss of Flow and Locked Rotor event include reactor coolant pump breaker position open (alarm and indicator light), reactor coolant pump overcurrent trip, and abnormal pump seal flow indications. Other event indications, not directly related to the failed pump, are: (1) Pressurizer safety relief valve (PSRV) indication system alarms when the Pressurizer power operated relief and safety valves open; (2) core exit thermocouples reading high; and (3) wide range Steam Generator water level indication low.

The Eagle 21 SER does not explicitly describe mitigation of this event if the PPS fails due to CCF. The existing FSARU Chapter 15 analysis states that RCS pressure is sufficient to lift the Pressurizer safety relief valves; however, no credit is taken for the Pressurizer pressure-high reactor trip as automatic backup to the PPS-generated RCS low flow trip function. In accordance with the guidance in NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the RCS Flow-Low reactor trip (2/3 Flow-Low in 2/4 loops > Permissive 7; 2/3 Flow-Low in any loop > Permissive 8) is generated in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

Although the existing FSARU Chapter 15 event analysis does not take credit for it, the Pressurizer pressure-high reactor trip generated in the diverse ALS portion of the replacement PPS provides additional diverse automatic backup to the RCS Flow-Low reactor trip for this event.

2. **Accidental Depressurization of the Reactor Coolant System**

FSARU Section 15.2.12 Accidental Depressurization of the Reactor Coolant System

An Accidental Depressurization of the RCS could occur as the result of an inadvertent opening of a Pressurizer relief or safety valve. Primary protection is provided by a reactor trip on a low Pressurizer pressure or OTDT signal. Both of these reactor trips are processed by the existing PPS. If the PPS fails, an automatic reactor trip may not occur for this event. Signals processed outside the PPS that would provide the operator with indication of an event are wide range containment pressure indicators, Pressurizer safety or relief valve position indication, high Pressurizer and safety valve discharge temperature (high reading), PSRV position indication system alarms, Pressurizer relief tank level, and PSRV acoustic monitor.

In accordance with the guidance in NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the Pressurizer Pressure-Low reactor trip function is generated in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

3. **Loss of Coolant Accidents – (Small and Large Break LOCA)**

FSARU Section 15.3.1 Loss of Reactor Coolant from Small Rupture Pipes or from Cracks in Large Pipes that Actuate Emergency Core Cooling System (Small Break LOCA)

FSARU Section 15.4.1 Major Reactor Coolant System Pipe Ruptures (Large Break LOCA)

A loss-of-coolant accident (LOCA) is defined as a rupture of the RCS piping or of any line connected to the system. Ruptures of small cross section (Small Break LOCA – SBLOCA) cause expulsion of the coolant at a rate that can be accommodated by the charging pumps that would maintain an operational water level in the Pressurizer permitting the operator to execute an orderly shutdown.

Should a larger break occur (Large Break LOCA – LBLOCA), depressurization of the RCS causes fluid to flow to the RCS from the Pressurizer resulting in a pressure and level decrease in the Pressurizer. Reactor trip occurs when the Pressurizer low-pressure trip setpoint is reached. The safety injection system (SIS) is actuated when the appropriate Pressurizer low-pressure setpoint is reached. Reactor trip and SIS actuation are also initiated by a high containment pressure signal.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the following functions are generated automatically in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

a) Pressurizer Pressure-Low-Low (ESFAS - Safety Injection)

b) Containment Pressure-High (ESFAS - Safety Injection, Phase A Containment Isolation)

c) Containment Pressure High-High Safeguards Actuation (ESFAS – Phase B Containment Isolation, Containment Spray in conjunction with Safety Injection)

4. Steam Line Break Events

FSARU Section 15.2.14 Accidental Depressurization of the Main Steam System

FSARU Section 15.4.2.1 Rupture of a Main Steam Line at Hot Shutdown

FSARU Section 15.4.2.3 Rupture of a Main Steam Line at Full Power

Reactor trip (at-power cases), safety injection and feedwater isolation are required to mitigate steam line break events. Sufficient reactor trip signals, from systems other than the replacement PPS, available as backup are: high neutron flux (all ranges, depending on initial power level) and high neutron positive flux rate. Borated coolant is automatically provided by the accumulators if the RCS pressure drops below the accumulator injection pressure. Additionally, the Diablo Canyon units have steam line check valves that prevent reverse flow from the unfaulted steam generators limiting the magnitude of the blowdown to the faulted steam generator.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the following functions are generated in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

a) Pressurizer Pressure-Low-Low (ESFAS – Safety Injection)

b) Containment Pressure-High (ESFAS – Safety Injection, Phase A Containment Isolation)

c) Containment Pressure High-High (ESFAS – Phase B Containment Isolation, Containment Spray coincident with Safety Injection)

5. FSARU 15.4.2.2 Major Rupture of a Main Feedwater Pipe

A major feedwater line rupture is defined as a break in a feedwater pipe large enough to prevent the addition of sufficient feedwater to the steam generators to maintain shell-side fluid inventory in the steam generators. Depending on the size of the break and the plant operating conditions at the time of the break, the break could cause either an RCS cooldown (by excessive energy discharge through the break), or an RCS heatup. Potential RCS cooldown resulting from a secondary pipe rupture is evaluated in Section 15.4.2.1. Therefore, only RCS heatup effects are evaluated for a feedline rupture.

A feedline rupture reduces the ability to remove heat generated by the core from the RCS. The following provide the necessary protection against a main feedwater line rupture:

- A reactor trip on any of the following conditions:
  - Pressurizer high pressure
  - OTDT
  - Steam generator low-low water level in any steam generator
- Safety injection signals from any of the following:
  - Steam line low pressure
  - Containment high pressure
- The AFW system provides decay heat removal

The diverse AMSAC trips the turbine and initiates secondary plant heat removal if the PPS does not trip the reactor due to loss of the secondary heat sink in accordance with 10 CFR 50.62 [9].

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, the following functions are generated in the independent, inherently diverse Class IE ALS portion of the proposed replacement PPS.

a) Pressurizer High Pressure (Reactor Trip)

b) Containment High Pressure (ESFAS – Safety Injection, Phase A Containment Isolation)

6. FSARU Section 15.4.3 Steam Generator Tube Rupture (SGTR)

Primary reactor protection for this event is provided by a reactor trip on OTDT. Backup reactor trip signals are generated by the Pressurizer low pressure, Turbine Trip on High Steam Generator Level Permissive 14 or Pressurizer low pressure SI signals. All of these protection signals are generated by the PPS. Safety injection is initiated via a low Pressurizer pressure signal, but is not required for core protection. Signals generated by systems other than the PPS are the main steam line, steam jet air ejector off-gas, steam generator blowdown (blowdown header and blowdown tank discharge), and plant vent radiation indicators and alarms. The operator would also notice a decrease in the volume control tank level and possibly an increase in the observed wide range steam generator water level (should the feedwater controller not respond to the decreased demand) which would also result in event indicators.

The RCS charging system will attempt to maintain Pressurizer level, accompanied by Pressurizer low pressure and low-level alarms. The operator's first indication of an SGTR event is the steam line, steam jet air ejector off-gas and/or steam generator blowdown radiation monitors. These radiation monitoring systems are diverse, with independent monitors and annunciators and would provide multiple indications of the event. Upon annunciation[1] of any of these signals, existing Diablo Canyon operating procedures provide the operator with the guidance necessary to effectively mitigate the SGTR event.

Existing DCPP procedures direct the operator in mitigation and recovery from this event. In the proposed replacement PPS, the OTDT reactor trip is generated in the Tricon and the Pressurizer Pressure-Low Reactor Trip and Pressurizer Pressure-Low-Low Safety Injection functions are generated in the inherently diverse ALS, which is not affected adversely by software CCF as described in Section 2.3.2, and provides automatic event mitigation to assist the operator.

3.2 Diverse Mitigating Functions for DCPP FSARU Chapter 15 Accident Analyses

This section evaluates, using engineering judgment, the impact on the DCPP FSARU Chapter 15 initiating events listed in Table 3-1 of replacing the existing Westinghouse Eagle 21 PPS with the proposed replacement PPS. The Tricon portion of the proposed replacement PPS is software-based; a CCF that disables Tricon-based protective functions is considered credible. The ALS portion of the proposed replacement PPS addresses CCF as described in Section 2.3.2 to meet the ISG-02 [3] Staff position. The diverse ALS cannot be affected by a Tricon CCF.

Table 3-6 lists each FSARU Chapter 15 event, and describes the diverse automatic mitigation functions (for which CCF is addressed as described in Section 2.3.2), and the diverse indications and manual controls that are not subject to a software CCF that could degrade the primary safety function.

The evaluation considered that the plant response to the postulated initiating events (PIE) with a concurrent postulated CCF can be addressed by one of the following approaches.

1. If the plant reaches a new steady-state condition without exceeding a safety limit, no protective function or immediate manual action is required.
2. The PIE is mitigated by an automatic protective function that is not degraded by the postulated CCF.
3. If the primary and backup automatic protective functions credited in the Eagle 21 diversity evaluation are degraded due to the postulated CCF, automatic Class IE mitigative action that is not affected adversely by software CCF is provided through the diverse ALS.

3.3 Manual Actuation and Control of Plant Critical Safety Functions

The Diablo Canyon protection system design includes displays and controls in the main control room for manual actuation and management of plant critical safety functions. Where necessary and practical, the indications are derived from the raw sensor signal and the indications are not processed by any digital

[1]With respect to the sensitivity of these monitors, a leak rate of greater than 1 gallon per day at DCPP will result in steam jet and air ejector off-gas indications.

system. The available displays and controls are listed in Table 3-5 and Table 3-6 and include but are not limited to the following:

1. Reactivity Control

   Reactor trip may be initiated at any time by controls that are entirely independent of the PPS [Figure 2-3]. Independent indication of rod position is provided as well. The Nuclear Instrumentation System provides diverse Class IE indication of neutron flux.

2. Reactor Core Cooling and Heat Removal

   The diverse AMSAC provides secondary plant heat removal should the reactor fail to trip. Auxiliary Feedwater may be initiated manually and monitored by controls that are independent of the PPS.

3. Reactor Coolant System Integrity

   Safety Injection may be initiated manually and monitored by controls that are independent of the PPS [Figure 2-4].

4. Containment Isolation and Integrity

   Containment Spray, Containment Isolation and Containment Ventilation Isolation may be initiated manually and monitored by controls that are independent of the PPS.

3.4 Conclusions

The Diablo Canyon Units 1 and 2 licensing basis accident analyses were reviewed to determine which events required the Process Protection System for primary or backup protection. Those events identified as requiring the PPS for primary protection system response were reviewed to determine if a timely diverse means of automatically mitigating the transient was available or annunciators and indicators were available to allow the operator to diagnose the event and bring the plant to a safe shutdown condition in a timely manner.

For most events, no operator action is required since sufficient non-PPS based automatic functions exist; i.e., the Nuclear Instrumentation System (NIS), Solid State Protection System (SSPS) and the AMSAC. For several events, however, some operator action was credited in the NRC Eagle 21 Safety Evaluation Report [13]. In these cases, backup protection system functions, alarms, and indicators processed independent of the PPS, along with existing Diablo Canyon operating procedures and Emergency Operating Procedures, were credited to bring the plant to a safe shutdown condition. Depending upon the event, operator action was required in ten minutes or less.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, where previous evaluations relied upon manual operator action to mitigate several such events, automatic mitigation functions are generated in the independent, inherently diverse ALS portion of the proposed replacement PPS for those events.

In effect, the proposed replacement PPS returns the Diablo Canyon Process Protection System configuration very similar to that described in the original diversity evaluation provided in WCAP 7306 [2]; that is, sufficient design defense in depth and diversity exists through monitoring numerous variables by different means that two or more diverse automatic protective actions terminate each FSARU Chapter 15 event that requires an automatic function before unacceptable consequences can occur. This also applies to the functions credited with manual operator action in the Eagle 21 SER to mitigate events that occurred with a concurrent postulated CCF to the PPS. That this conclusion applies to the proposed replacement PPS is demonstrated in Table 3-6, which assumes that CCF disables the computer-based Tricon portion of the replacement PPS while the logic-based ALS portion of the replacement PPS is not affected adversely by software CCF as described in Section 2.3.2, and remains available to perform safety functions automatically.

Therefore, the inherent diversity provided by the logic-based ALS portion of the proposed replacement PPS ensures that all accidents and events credited with automatic PPS mitigation in Diablo Canyon FSARU Chapter 15 analyses continue to be mitigated automatically with a concurrent software CCF. Thus, the proposed PPS provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

This page left blank by intent

Table 3-1 DCPP FSARU Chapter 15 Safety Analysis Events and Mitigating Functions

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Condition II – Faults of Moderate Frequency	**15.2**		
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from Subcritical Condition	15.2.1	Power-Range High-Flux (Low Setting) RT	• Source-Range High-Flux RT • Intermediate-Range High-Flux RT • Power-Range High-Flux (High Setting) RT • Power-Range Flux Positive Rate RT
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	15.2.2	• Power-Range High-Flux (High Setting) RT • OTDT RT	• Power-Range Flux High Positive Rate RT • OPDT RT • Pressurizer High-Pressure RT • Pressurizer High-Level RT
Rod Cluster Control Assembly Misoperation	15.2.3	As Currently Licensed, Operators Rely on Indications Outside PPS to Mitigate This Event.	NA
Uncontrolled Boron Dilution (During Refueling)	15.2.4	Operator action – terminate dilution	NA
Uncontrolled Boron Dilution (During Startup)	15.2.4	Source-Range High-Flux RT	• Intermediate-Range High-Flux RT • Power-Range High Flux (Low Setting) RT
Uncontrolled Boron Dilution (At Power) Reactor Manual	15.2.4	Operator Action – Terminate Dilution • Low Rod Insertion Alarm • Low-Low Rod Insertion Alarm	NA
Uncontrolled Boron Dilution (At Power) Reactor Auto	15.2.4	• Power-range high flux (high setting) RT • OTDT RT	• OPDT RT • Pressurizer High-Pressure RT • Pressurizer High-Level RT

Table 3-1 DCPP FSARU Chapter 15 Safety Analysis Events and Mitigating Functions, Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Partial Loss of Forced Reactor Coolant Flow (No automatic protection below Permissive 7)	15.2.5	• 2/3 RCS Flow-Low In Any Loop RT Above Permissive 8 (35% NI)[2] • 2/3 RCS Flow-Low In 2/4 Loops RT Above Permissive 7 (10% NI)	• None credited for single loop loss of flow • 2/4 RCP Breaker Open Position above Permissive 7 provides backup for loss of flow in more than one loop[3]
Startup of an Inactive Reactor Coolant Loop	15.2.6	Event Precluded By Technical Specifications	Not Applicable
Loss of External Electrical Load and/or Turbine Trip	15.2.7	• Pressurizer High-Pressure RT • OTDT RT	• Pressurizer High Level RT • OPDT • RT on TT (turbine trip only)
Loss of Normal Feedwater Flow	15.2.8	• SG Low-Low Level RT and AFW Actuation	• Pressurizer High Pressure RT • Pressurizer Level High • OTDT
Loss of Non-Emergency AC Power to the Station Auxiliaries	15.2.9	• RT on TT • SG Low-Low Level AFW Actuation	• Pressurizer High Pressure RT • Pressurizer High Level RT • OTDT RT • Reactor Coolant Pump UV RT • 2/4 RCP Breaker Open Position RT above Permissive 7
Excessive Heat Removal Due to Feedwater System Malfunctions	15.2.10	• SG High-High Level TT and FWI • RT on TT (not required for core protection)	• Power-Range High-Flux (High or Low Setting) RT • OTDT RT • OPDT RT

[2] The Reactor Coolant Flow-Low Reactor Trip function provides primary protection for the Partial Loss of Forced Reactor Coolant Flow event (Section 15.2.5). Although available, the diverse Reactor Coolant circuit breaker open reactor trip functions do not provide automatic protection for single loop RCS low flow events.

[3] Reactor trip on reactor coolant pump breaker position open provides backup protection for 2 or 3 out of 4 loop Partial Loss of Reactor Coolant Flow events. Since this reactor trip logic requires signals from at least 2 out of 4 reactor coolant pumps, it does not provide an automatic reactor trip for a 1 out 4 loop loss of flow.

Table 3-1 DCPP FSARU Chapter 15 Safety Analysis Events and Mitigating Functions, Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Sudden Feedwater Temperature Reductions	15.2.11	None Required – Event precluded by elimination of Load Transient Bypass (LTB) function.	None Required
Excessive Load Increase Incident	15.2.12	None Required[4]	• OTDT RT • OPDT RT • Power-Range High-Flux RT (High or Low Setting)
Accidental Depressurization of the Reactor Coolant System	15.2.13	OTDT RT	Pressurizer Low-Pressure RT
Accidental Depressurization of the Main Steam System	15.2.14	Pressurizer Low Pressure SI	• Steam Line Low Pressure SI • OPDT • Power Range High Flux RT (High or Low Setting)
Spurious Operation of the Safety Injection System	15.2.15.1	Operator Action – Terminate SI	Pressurizer Low-Pressure RT
Condition III – Infrequent Faults	**15.3**		
Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes that Actuate Emergency Core Cooling Systems	15.3.1	• Pressurizer Low-Pressure RT • Pressurizer Low Pressure SI/RT	Containment Pressure High SI/RT
Minor Secondary System Pipe Breaks	15.3.2	Bounded by Main Steam Line Rupture analysis (Section 15.4.2.1); explicit analysis not performed	NA

[4] Reactor trip does not occur for any of the cases analyzed. The plant reaches a new equilibrium condition at a higher power level corresponding to the increase in steam flow.

Table 3-1 DCPP FSARU Chapter 15 Safety Analysis Events and Mitigating Functions, Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	15.3.3	None required	Core loading administrative procedures contain controls to prevent fuel assembly loading errors. Errors will be detected by the Moveable Incore Detector System (MIDS); or will cause a sufficiently small perturbation to be acceptable within the uncertainties allowed between nominal and design power shapes.
Complete Loss of Forced Reactor Coolant Flow (No automatic trip below Permissive 7)	15.3.4	Above Permissive 7 (10% NI) • RCP undervoltage RT (both buses) • RCP underfrequency RT (either bus)	• 2/4 RCP Breaker Open Position RT above Permissive 7 • 2/3 RCS Flow-Low in 2/4 Loops RT above Permissive 7[5] • 2/3 RCS Flow-Low in Any Loop RT above Permissive 8 (35% NI)[4]
Single Rod Cluster Control Assembly Withdrawal at Full Power	15.3.5	OTDT RT	• Power-Range High Flux (High Setting) RT • Power-Range Flux Positive Rate RT
Condition IV – Limiting Faults	**15.4**		
Major Reactor Coolant System Pipe Rupture (LBLOCA)	15.4.1	• Pressurizer Low Pressure RT • Pressurizer Low Pressure SI	Containment Pressure High ESF (SI/RT)
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line at Hot Shutdown	15.4.2.1	• Steam Line Low Pressure SI • Containment High Pressure SI	• Pressurizer Low Pressure SI • High Negative Steam Line Pressure Rate (SLI)

[5] The Reactor Coolant Flow-Low Reactor Trip function provides primary protection for the single reactor coolant pump locked rotor event (Section 15.4.4). It provides backup protection to the UV/UF and RCP circuit breaker open reactor trip functions for the complete loss of forced reactor coolant flow event..

Table 3-1 DCPP FSARU Chapter 15 Safety Analysis Events and Mitigating Functions, Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Major Secondary Pipe Rupture – Major Rupture of a Main Feedwater Pipe	15.4.2.2	• Steam Generator Level Low-Low RT and AFW actuation	• Pressurizer High-Pressure RT • OTDT RT • SI/RT on: o Steam Line Low-Pressure o High Containment Pressure
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line at Full Power	15.4.2.3	• Steam Line Low Pressure SI/RT • OPDT RT	• Pressurizer Low Pressure SI
Steam Generator Tube Rupture	15.4.3	• OTDT RT	• Pressurizer Low-Pressure RT • Steam Generator High Level Permissive 14 TT/RT • Pressurizer Low-Pressure SI/RT
Single Reactor Coolant Pump Locked Rotor	15.4.4	• 2/3 RCS Flow-Low in any Loop RT above Permissive 8 (35% NI)	• Pressurizer High Pressure RT
Fuel Handling Accident	15.4.5	• None required	• Not Applicable
Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection	15.4.6	• Power-Range High Flux (High or Low Setting) RT	• Source-Range High-Flux RT • Intermediate-Range High-Flux RT • Power-Range Flux Positive Rate RT
Rupture of a Waste Gas Tank	15.4.7	• None required	• Not Applicable
Rupture of a Liquid Holdup Tank	15.4.8	• None required	• Not Applicable
Rupture of Volume Control Tank	15.4.9	• None required	• Not Applicable
Steam Line Break Inside Containment (Containment Heat Removal)	6.2.2	• Steamline Low Pressure • Pressurizer Low Pressure	• Containment High-High Pressure • Containment High Pressure

Table 3-2 Safety Analysis Events That Do Not Require PPS for Primary or Backup Protection (Category 1 Events)

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Condition II – Faults of Moderate Frequency	**15.2**		
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from Subcritical Condition	15.2.1	Power-Range High-Flux (Low Setting) RT	NIS trips are not subject to software CCF and are available(2): • Source-Range High-Flux RT • Intermediate-Range High-Flux RT • Power-Range High-Flux (High Setting) RT • Power-Range Flux Positive Rate RT
Rod Cluster Control Assembly Misoperation	15.2.3	Power Range Neutron Flux	None required per FSARU. Plant reaches a new steady-state condition without exceeding a safety setpoint.
Uncontrolled Boron Dilution (During Refueling)	15.2.4	Operator Action – Terminate Dilution	None Required Per FSARU
Uncontrolled Boron Dilution (During Startup)	15.2.4	Source-Range High-Flux RT	NIS trips are not subject to software CCF and are available[6] • Intermediate-Range High-Flux RT • Power-Range High Flux (Low Setting) RT
Uncontrolled Boron Dilution (At Power) Reactor Manual	15.2.4	Operator Action – Terminate Dilution; Notified by: • Low Rod Insertion Alarm • Low-Low Rod Insertion Alarm	None Required Per FSARU
Startup of an Inactive Reactor Coolant Loop	15.2.6	Event is precluded by Tech Spec requirements	None required.
Sudden Feedwater Temperature Reductions	15.2.11	None Required – Load Transient Bypass (LTB) function has been eliminated. Bounded by Excessive Load Increase (FSARU 15.2.12)	None Required Per FSARU

[6] The FSARU Section 15.2.12 analysis demonstrates that normal reactor control systems and engineered safety systems are not required to function. The reactor protection system is assumed to be operable; however, reactor trip is not encountered for most cases due to the error allowances assumed in the setpoints. In the event of software-related CCF, the OPDT and OTDT reactor trips may not be available.

Table 3-2 Safety Analysis Events That Do Not Require PPS for Primary or Backup Protection (Category 1 Events), Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Excessive Load Increase Incident[7]	15.2.12	For all cases, the plant rapidly reaches a stabilized condition at the higher power level. Normal plant operating procedures would then be followed to reduce power. Reactor trip does not occur for any of the cases analyzed	• Power-Range High-Flux RT (High or Low Setting) • OTDT RT • OPDT RT
Condition III – Infrequent Faults	**15.3**		
Inadvertent Loading and Operation of a Fuel Assembly an in Improper Position	15.3.3	• None required. Adequate measurements are taken to detect the existence of an improperly loaded fuel assembly.	• None required.
Complete Loss of Forced Reactor Coolant Flow (No automatic trip below Permissive 7)	15.3.4	Above Permissive 7 (10% NI) • RCP undervoltage RT (both buses) • RCP underfrequency RT (either bus)	• 2/4 RCP Breaker Open Position RT above Permissive 7 • 2/3 RCS Flow-Low in 2/4 Loops RT above Permissive 7 • 2/3 RCS Flow-Low in Any Loop RT above Permissive 8 (35% NI)[8]

[7] The FSARU analysis of this event does not require a primary mitigating function. The diverse high flux trips and the PPS functions provide backup in the unlikely event that a reactor trip is required.

[8] The Reactor Coolant Flow-Low Reactor Trip function provides primary protection for the single reactor coolant pump locked rotor event (Section 15.4.4). It provides backup protection to the UV/UF and RCP circuit breaker open reactor trip functions for the complete loss of forced reactor coolant flow event.

Table 3-2 Safety Analysis Events That Do Not Require PPS for Primary or Backup Protection (Category 1 Events), Continued

Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Condition IV – Limiting Faults	**15.4**		
Fuel Handling Accident	15.4.5	Not applicable, radiological release calculation only.	
Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection	15.4.6	NIS trips are not subject to software CCF and are available • Power-Range High Flux (High or Low Setting) • Source-Range High-Flux • Intermediate-Range High-Flux • Power-Range Flux Positive Rate	• Wide Range Reactor Coolant System Pressure • Pressurizer Safety Valves
Rupture of a Waste Gas Tank	15.4.7	Not applicable, radiological release calculation only.	
Rupture of a Liquid Holdup Tank	15.4.8	Not applicable, radiological release calculation only.	
Rupture of Volume Control Tank	15.4.9	Not applicable, radiological release calculation only.	

Table 3-3 Safety Analysis Events with Diverse Automatic Primary Safety Function Actuation That Require PPS for Backup Protection (Category 2 Events)

Postulated Initiating Event	FSARU Section	Primary Mitigating Function	Backup Mitigating Function
Uncontrolled Boron Dilution (At Power) Reactor Auto	15.2.4	• Power-range high flux (high setting) RT • OTDT RT	• Power-Range Flux High Positive Rate RT • OPDT RT • Pressurizer High-Pressure RT • Pressurizer High-Level RT
Spurious Operation of the Safety Injection System	15.2.15.1	Operator Action – Terminate SI	Pressurizer Low Pressure SI/RT

Table 3-4 Safety Analysis Events That Require Process Protection System Channels for Primary Safety Function Actuation But Have Available Diverse Automatic Backup (Category 3 Events)

Event	Primary Safety Signal	Function	Backup Safety Signal	Function
Uncontrolled Rod Cluster Control Assembly (RCCA) Bank Withdrawal at Power (FSARU 15.2.2)	OTDT	RT[9, 10]	High Neutron Flux – Power Range	RT
Loss of Non-Emergency AC Power to the Station Auxiliaries FSARU 15.2.9)	• RT on TT[11] • SG Low-Low Level AFW Actuation	RT	• Reactor Coolant Pump UV • 2/4 RCP Breaker Open Position RT above Permissive 7 • Pressurizer High Pressure • Pressurizer High Level • OTDT	RT
Excessive Heat Removal due to Feedwater Malfunctions[12] (FSARU 15.2.10)	• Steam Generator High Level Permissive 14	TT/RT/ FLI	• OTDT • OPDT • High Power Range Neutron Flux	RT
Single RCCA Withdrawal at Full Power (FSARU 15.3.5[9]	Operator Action Alerted by: • RCCA Withdrawal Alarm • Rod Deviation Alarm • Urgent Rod Control Failure Alarm	Terminate Rod Withdrawal	NA	NA

[9] Primary protection signal depends on the reactivity insertion rate. In general for slower reactivity insertion rates the primary reactor trip signal occurs on OTDT, while for faster reactivity insertion rates the primary reactor trip signal is on HNF-Power Range.

[10] Depending on initial bank insertion and location of the withdrawn RCCA, automatic reactor trip may not occur sufficiently fast to prevent the minimum core DNBR from falling below the safety limit value. Evaluation of this case at the power and coolant condition at which OTDT trip would be expected to trip the plant shows that an upper limit for the number of rods with a DNBR less than the safety limit value is 5 percent.

[11] Below 50% power (Permissive 9) a reactor trip does not automatically occur on a turbine trip signal.

[12] Primary reactor trip signal depends on initial accident conditions.

Table 3-5 Safety Analysis Events That Use Process Protection System Channels for Both Primary and Backup Safety Function Actuation (Category 4 Events)

Event	Primary Safety Signal	Function	Backup Safety Signal	Function	Diverse (Non-PPS) Protection, Indicators and Alarms
Partial Loss of Forced Reactor Coolant Flow (No automatic protection below Permissive 7) (FSARU 15.2.5)	RCS Low Flow[13] (2/3 Flow-Low in 2/4 loops > Permissive 7; 2/3 Flow-Low in 1/4 loops > Permissive 8)	RT	None Credited (for single loop loss of flow) 2/4 RCP Breaker Open Position above Permissive 7 provides backup for loss of flow in more than one loop	NA	Indication • Reactor Coolant Pump Circuit Breaker Position • Reactor Coolant Pump Overcurrent Trip • Wide Range Reactor Coolant System Pressure • Pressurizer Safety Relief Valve Position • Pressurizer Relief & Safety Discharge Temp. • Core Exit Thermocouples (high) • Wide Range Steam Generator Level (low)
Loss of External Electrical Load and/or Turbine Trip (FSARU 15.2.7)	• Pressurizer High-Pressure RT • OTDT RT	RT	• Pressurizer High Level RT • OTDT	RT	RT on TT (turbine trip only)[14]
Loss of Normal Feedwater (FSARU 15.2.8)	• Steam Generator Narrow Range Low-Low Level	RT/AFW	• Pressurizer High Pressure RT • Pressurizer Level High • OTDT	RT	Protection • AMSAC Indication • Steam Generator Wide Range Level • Reactor Coolant System Wide Range Pressure
Accidental Depressurization of the Reactor coolant System (FSARU 15.2.13)	Pressurizer Low Pressure	RT	OTDT	RT	Indication • Wide Range Containment Pressure • Pressurizer Relief & Safety Valve Pos. • Pressurizer Relief & Safety Discharge Temp.

[13] The Reactor Coolant Flow-Low Reactor Trip function provides primary protection for the Partial Loss of Forced Reactor Coolant Flow event (Section 15.2.5). Although available, the diverse Reactor Coolant circuit breaker open reactor trip functions do not provide automatic protection for single loop RCS low flow events.

[14] Below 50% power (Permissive 9) a reactor trip does not automatically occur on a turbine trip signal. AMSAC is not available below C-20 (40% RTP) per the AMSAC safety evaluation.

Table 3 -5 Safety Analysis Events That Use Process Protection System Channels for Both Primary and Backup Safety Function Actuation (Category 4 Events), Continued

Events	Primary Safety Signal	Function	Backup Safety Signal	Function	Diverse (Non-PPS) Protection, Indicators and Alarms
Accidental Depressurization of the Main Steam System.[15] (FSARU 15.2.14)	Pressurizer Low Pressure	RT/ ESF	OPDT Steam Line Low Pressure High Rate RT on ESF	RT ESF RT	Protection • High Power Range Neutron Flux – RT • Steam Line Low Pressure – ESF Indication • Reactor Water Storage Tank Level Indicator and Alarm • Steam Generator Safety Valve or Steam Dump Pos. Indication • Wide Range Steam Generator Level (low) • Core Exit Thermocouples (low)
Loss of Coolant Accident[16] (FSARU 15.3.1) (FSARU 15.4.1)	Pressurizer Low Pressure	ESF/ RT	Containment High-High Pressure Containment High Pressure RT on ESF	ESF ESF RT	Protection • RCP Overcurrent Protection Indication • Containment Radiation Monitors • Reactor Water Storage Tank Level Indicator and Alarm • Containment Sump Level • Core Exit Thermocouples (High) • Accumulator Level and Pressure (Low) • Containment Temperature (High) • Volume control Tank Level (low) • Subcooling Margin (Low, Low-Low) • Control Rod Drive Mechanism Fan Suction Temperature (High)

[15] An automatic reactor trip is not required for core protection. Feedwater isolation is required to prevent excessive moisture carryover to the turbine and water in the steam pipes (which could cause a steam line break event). Automatic actuation of feedwater isolation is not available outside the PPS. Indications are available to the operator to alert this condition for manual control.

[16] Large Break LOCA analysis assumes that the rods do not drop.

Table 3 -5 Safety Analysis Events That Use Process Protection System Channels for Both Primary and Backup Safety Function Actuation (Category 4 Events), Continued

Event	Primary Safety Signal	Function	Backup Safety Signal	Function	Diverse (Non-PPS) Protection, Indicators and Alarms
Minor Secondary System Pipe Breaks (FSARU 15.3.2)	Bounded by Main Steam Line Rupture analysis (Section 15.4.2.1); explicit analysis not performed				
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line at Hot Shutdown (FSARU 15.4.2.1)	• Steam Line Low Pressure • Containment High Pressure	SI SI	• Pressurizer Low Pressure • High Negative Steam Line Pressure Rate	SI SLI	Indication • Wide Range Steam Generator Level • Reactor Water Storage Tank Level Indicator and Alarm • Core Exit Thermocouples (Low) • Accumulator Level & Press. Indicators
Major Rupture of a Main Feedwater Pipe (FSARU 15.4.2.2)	Steam Generator Narrow Range Low-Low Level	RT/AFW	• Pressurizer High-Pressure • OTDT • Steam Line Low-Pressure • High Containment Pressure	RT RT SI/RT SI/RT	Protection • AMSAC • RT on TT Indication • Wide Range Steam Generator Level (Low) • Subcooled Margin Monitor (Low) • Containment Sump Level (High) • Core Exit Thermocouples (High) • Pressurizer Relief Tank Level (High) • Pressurizer Safety Relief Valve Position (Acoustic Monitors) • Stem Leakoff Temperature (High)

Table 3 -5 Safety Analysis Events That Use Process Protection System Channels for Both Primary and Backup Safety Function Actuation (Category 4 Events), Continued

Event	Primary Safety Signal	Function	Backup Safety Signal	Function	Diverse (Non-PPS) Protection, Indicators and Alarms
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line at Full Power (FSARU 15.4.2.3)	• Steam Line Low Pressure • OPDT RT	SI/RT RT	• Containment High-High Pressure • Pressurizer Low Pressure • Containment High Pressure	SLI ESF SI	Indication • Wide Range Steam Generator Level • Reactor Water Storage Tank Level Indicator and Alarm • Core Exit Thermocouples (Low) • Accumulator Level & Press. Indicators
Steam Generator Tube Rupture (FSARU 15.4.3)	OTDT	RT	• Pressurizer Low Pressure • Steam Generator High Level Permissive 14 • Pressurizer Low Pressure	RT RT on TT ESF	Indication • Wide Range Reactor Coolant System Pressure • Wide Range Steam Generator Level • Condenser air ejector radiation • Steam Generator blowdown steam line radiation
Single Reactor Coolant Pump Locked Rotor (FSARU 15.4.4)	Reactor Coolant System Low Flow[17]	RT	• Pressurizer High Pressure	RT	Indication • Reactor Coolant Pump Circuit Breaker Position • Reactor coolant Pump Overcurrent Trip • Wide Range Reactor Coolant System Pressure • Pressurizer Relief & Safety Valve Pos. • Pressurizer Relief & Safety Discharge Temp. • Core Exit Thermocouples (High) • Wide Range Steam Generator Level (low)

[17] The Reactor Coolant Flow-Low Reactor Trip function provides primary protection for the single reactor coolant pump locked rotor event (Section 15.4.4). Although available, the diverse Reactor Coolant circuit breaker open reactor trip functions do not provide automatic protection for single loop RCS low flow events.

Table 3 -5 Safety Analysis Events That Use Process Protection System Channels for Both Primary and Backup Safety Function Actuation (Category 4 Events), Continued

Event	Primary Safety Signal	Function	Backup Safety Signal	Function	Diverse (Non-PPS) Protection, Indicators and Alarms
Steam Line Break Inside Containment[18, 19] (FSARU 6.2.2 – Containment Heat Removal)	Steamline Low Pressure Pressurizer Low Pressure	ESF RT	Containment High-High Pressure Containment High Pressure	SLI/CS (coincident with SI) SI	Protection • High Power Range Neutron Flux • High Positive Neutron Flux Rate Indication • Wide Range Steam Generator Level • RWST Level Indicator and Alarm • Core Exit Thermocouples (Low) • Accumulator Level & Press. Indicators

[18] Steam line break cases analyzed at power, without PPS functions, would receive high neutron flux reactor trip signals (Nuclear Instrumentation System).
[19] The FSARU analysis assumes Old Steam Line Break Protection, which is conservative for plants such as DCPP with New Steam Line Break Protection Systems.

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator[2]	Diverse MCR Controls Available to Operator[3]
Condition II – Faults of Moderate Frequency	**15.2**			
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical Condition	15.2.1			
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	15.2.2			
Rod Cluster Control Assembly Misoperation	15.2.3			
Uncontrolled Boron Dilution (During Refueling)	15.2.4			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Uncontrolled Boron Dilution (During Startup)	15.2.4			
Uncontrolled Boron Dilution (At Power)	15.2.4			
Partial Loss of Forced Reactor Coolant Flow	15.2.5			
Loss of External Electrical Load and/or Turbine Trip	15.2.7			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Initiating Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Loss of Normal Feedwater Flow	15.2.8			
Loss of Non-Emergency AC Power to the Station Auxiliaries	15.2.9			
Excessive Heat Removal Due to Feedwater System Malfunctions	15.2.10			
Sudden Feedwater Temperature Reduction	15.2.11			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Excessive Load Increase Incident	15.2.12			
Accidental Depressurization of the Reactor Coolant System	15.2.13			
Accidental Depressurization of the Main Steam System	15.2.14			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Spurious Operation of the Safety Injection System at Power	15.2.15			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Update Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Condition III – Faults of Moderate Frequency	**15.3**			
Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes that Actuate Emergency Core Coolant System	15.3.1			
Minor Secondary System Pipe Breaks	15.3.2			
Inadvertent Loading and Operation of a Fuel Assembly an in Improper Position	15.3.3			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Update Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Complete Loss of Forced Reactor Coolant Flow (No automatic protection below Permissive 7)	15.3.4			
Single Rod Cluster Control Assembly Withdrawal at Full Power	15.3.5			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Condition IV – Limiting Faults	**15.4**			
Major Reactor Coolant System Pipe Ruptures (LOCA)	15.4.1			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator[(2)]	Diverse MCR Controls Available to Operator[(3)]
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line (zero power)	15.4.2.1			
Major Secondary System Pipe Rupture – Major Rupture of a Main Feedwater Pipe	15.4.2.2			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Event Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Major Secondary System Pipe Rupture – Rupture of a Main Steam Line at Full Power	15.4.2.3			
Steam Generator Tube Rupture (SGTR)	15.4.3			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Single Reactor Coolant Pump Locked Rotor	15.4.4			
Fuel Handling Accident	15.4.5			
Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection)	15.4.6			
Rupture of a Waste Gas Tank	15.4.7			
Rupture of a Liquid Holdup Tank	15.4.8			
Rupture of Volume Control Tank	15.4.9			

a

Table 3-6 Diverse Automatic Mitigating Functions, Indications and Manual Controls for Chapter 15 Events Following a Postulated CCF, Continued

Event	FSARU Section	Diverse Automatic Mitigating Function	Diverse MCR Indications Available to Operator(2)	Diverse MCR Controls Available to Operator(3)
Steam Line Break Inside Containment (Containment Heat Removal)	6.2.2			

a

Notes:

1 Deleted

2 For all events, manual RCS boron concentration sampling capability is required to verify shutdown margin for plant recovery.

3 For all events, the ability to maintain SG water level is required for plant recovery. In addition, RCS long term shutdown margin maintenance (emergency boration) is required.

4 Deleted

5 Parameter indication on MCB is isolated at replacement PPS input; not affected by CCF.

This page left blank by intent

4.0 Abbreviations and Acronyms

52HF15	4 KV Switchgear Bus "F" Breaker 15 (DCPP Unit 1 SI Pump 1)
AFW	Auxiliary Feedwater
ALS	Advanced Logic system
AMSAC	ATWS Mitigation System Actuation Circuitry
ANS	American Nuclear Society
ATWS	Anticipated Transient Without SCRAM
BTP	Branch Technical Position
BYA	Bypass Reactor Trip Breaker A
BYB	Bypass Reactor Trip Breaker B
CC1	Main Control Room Control Console Section 1 (Reactor Control)
CC2	Main Control Room Control Console Section 2 (Demin & Makeup Water)
CCF	Common Cause Failure
CLI	Current Loop Isolator
CNAC	Main Control Room Control Board Accumulator Service (VB2)
CNSI	Main Control Room Control Board Safety Injection (VB1)
CNV	Main Control Room Control Board Chemical & Volume Control System (VB2)
CRDM	Control Rod Drive Mechanism
CS	Containment Spray
CS	Control Switch [Figure 2-3 and Figure 2-4]
D3	Diversity and Defense-in-Depth
DAC	Digital-to-Analog Converter
DAS	Diverse Actuation System
DCPP	Diablo Canyon Power Plant
DDC	Digital-Digital Converter
DFP	Digital Filter Processor
DFWCS	Digital Feedwater Control System
DI&C	Digital Instrument & Control
DLH	Data Link Handler
DNBR	Departure from Nucleate Boiling Ratio
DTTA	Delta-T Taverage
EAI	Eagle Analog Input
EAO	Eagle Analog Output
ECO	Eagle Contact Output
E/I	Voltage to Current Converter
EPRI	Electric Power Research Institute
EPT	Eagle Partial Trip
ERFDS	Emergency Response Facility Data System
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FLB	Feedwater Line Break
FPGA	Field Programmable Gate Array
FSARU	Final Safety Analysis Report Update
FW	Feedwater
FWI	Feedwater Isolation
FWM	Feedwater Malfunction
HFE	Human Factors Engineering
HNF	High Neutron Flux
HMI	Human Machine Interface

I&C	Instrument & Control
I/E	Current to Voltage Converter
IEEE	Institute of Electrical and Electronic Engineers
IR	Intermediate Range
ISG	Interim Staff Guidance
ISLN/ISOL	Isolation
LAR	License Amendment Request
LBLOCA	Large Break LOCA
LCP	Loop Calculation Processor
LLC	Limited Liability Corporation
LOCA	Loss of Coolant Accident
LOF	Loss of Flow
LOL	Loss of Load
LONF	Loss of Normal Feedwater
LOOP	Loss of Offsite Power
LR	Locked rotor
LTB	Load Transient Bypass
LTOPS	Low Temperature Overpressure Protection System
MAS	Main Annunciator System
MCB	Main Control Board
MCR	Main Control Room
MFW	Main Feedwater
M-G	Motor Generator
MIDS	Moveable Incore Detector System
MSFIS	Main Steam and Feedwater Isolation System
MSS	Main Steam System
MVDU	Maintenance Video Display Unit
NI	Nuclear Instrumentation
NIS	Nuclear Instrumentation System
NR	Narrow Range
NRC	United States Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OPDT	Overpower Delta Temperature
OTDT	Overtemperature Delta Temperature
PAM	Post Accident Monitoring
PG&E	Pacific Gas & Electric Co.
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PLOF	Partial Loss of Flow
PORV	Power Operated Relief Valve
PPC	Plant Process Computer
PPS	Process Protection System
PR	Power Range
PSRV	Pressurizer Safety Relief Valve
PT	Potential Transformer
PWR	Pressurized Water Reactor
PZR	Pressurizer
RC	Reactor Coolant
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump

RCS	Reactor Coolant System
RHR	Reactor Heat Removal
RMU	Reactor Makeup
RNARA	Nuclear Auxiliary Relay Rack A DCPP Electric Equipment Code Designation
RNARB	Nuclear Auxiliary Relay Rack BDCPP Electric Equipment Code Designation
RNSLA	SSPS Logic Rack A DCPP Electric Equipment Code Designation
RNSLB	SSPS Logic Rack B DCPP Electric Equipment Code Designation
RPS	Reactor Protection System
RT	Reactor Trip
RTA	Reactor Trip Circuit Breaker "A"
RTB	Reactor Trip Breaker
RTD	Resistance Temperature Detector
RTP	Reactor Thermal Power
RTS	Reactor Trip System
RWAP	Rod Withdrawal at Power
RWST	Reactor Water Storage Tank
SBLOCA	Small Break LOCA
SER	Safety Evaluation Report
SG	Steam Generator
SGL	Steam Generator Level
SGTR	Steam Generator Tube Rupture
SHF15	4 KV Switchgear Bus "F" Cubicle 15 (DCPP Unit 1 SI Pump 1)
SI	Safety Injection
SIS	Safety Injection Signal
SL	Steam Line
SLB	Steam Line Break
SLI	Steam Line Isolation
SRP	Standard Review Plan
SR	Source Range
SSI	Spurious Safety Injection
SSPS	Solid State Protection System
Tavg	Average Reactor Coolant Temperature
Tc	Cold Leg Reactor Coolant Temperature
TC	Circuit Breaker Trip Coil
Th	Hot Leg Reactor Coolant Temperature
TMR	Triple Modular Redundant
TSP	Test Sequence Processor
TT	Turbine Trip
TWG	Task Working Group
UF	Underfrequency
UV	Undervoltage
UVXA	Undervoltage Auxiliary Relay "A"
VB1	Main Control Room Vertical Control Board Section 1
VB2	Main Control Room Vertical Control Board Section 2
VCT	Volume Control Tank
WCAP	Westinghouse Commercial Atomic Power
WCNOC	Wolf Creek Nuclear Operating Company
WR	Wide Range

This page left blank by intent

5.0 References

1. Diablo Canyon Power Plant Final Safety Analysis Report (FSARU)
2. WCAP-7306, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, Westinghouse Electric Corporation, 1969 (Non-Proprietary Class 3)
3. Digital Instrumentation and Controls DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance Revision 2, June 5, 2009
4. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," October 1994
5. NUREG-0800, "Standard Review Plan," Chapter 7, Appendix 7-1C, Revision 5, March 2007
6. Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1 published as EPRI TR-1000799, "Generic Qualification of the Triconex Corporation TRICON Triple Modular Redundant Programmable Logic Controller System for Safety-Related Applications in Nuclear Power Plants," November 2000
7. Letter from Stuart A. Richards (NRC) to Troy Martel (Triconex Corporation), "Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1" December 11, 2001 published as EPRI TR-1003114 ADAMS Accession Number ML013470433
8. Letter No. NRC-V10-09-01, J. Polcyn (Invensys) to NRC, "Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and "Application for withholding Proprietary Information from Public Disclosure," dated September 9, 2009
9. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"
10. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"
11. NRC, Safety Evaluation Report Wolf Creek Nuclear Operating Company (WCNOC) Main Steam and Feedwater Isolation System (MSFIS), ADAMS Accession Number ML090610317
12. ALS Platform Overview, 6002-00026, CS Innovations, LLC, Rev 1, July, 2008
13. NRC, "Safety Evaluation Report Eagle 21 Reactor Protection System Modification With Bypass Manifold Elimination, PG&E, Diablo Canyon Power Plant, " (October 7, 1993)
14. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," March 2007
15. DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms - Communications Issues (HICRc), Revision 1, March 6, 2009

This page left blank by intent